Guía Técnica Ampliada de Redes y Telecomunicaciones

Este documento proporciona una base de conocimiento extensa y estructurada sobre los conceptos, tecnologías, protocolos y herramientas esenciales utilizadas en redes y telecomunicaciones. Su objetivo es servir como una fuente sólida y detallada para agentes RAG, estudiantes, administradores de red, ingenieros y asistentes especializados en configuración, diagnóstico y análisis de entornos de red tanto a nivel empresarial como doméstico.

1. Fundamentos de Redes

Definición
Una red de computadoras es un sistema formado por múltiples dispositivos interconectados que intercambian información entre sí mediante distintos medios de comunicación. Estos dispositivos pueden compartir datos, recursos físicos y servicios, como impresoras, servidores, acceso a Internet o aplicaciones distribuidas.

Tipos de Redes
Existen diversas categorías de redes, clasificadas según su alcance, tamaño y propósito:

- PAN (Personal Area Network): red de corto alcance, usada para conectar dispositivos personales como teléfonos, relojes inteligentes, audífonos o periféricos.
- LAN (Local Area Network): red dentro de un edificio o casa, con alta velocidad y baja latencia.
- MAN (Metropolitan Area Network): red intermedia que abarca una región urbana o campus universitario.
- WAN (Wide Area Network): cubre grandes distancias geográficas. Su mayor ejemplo es Internet.
- WLAN: versión inalámbrica de una LAN, sustentada en tecnologías como Wi-Fi.
- CAN (Campus Area Network): red de campus, utilizada para conectar múltiples edificios dentro de una institución.
- SAN (Storage Area Network): red especializada para almacenamiento de alto rendimiento.

Componentes Principales de una Red
Una red incluye múltiples dispositivos que cumplen funciones específicas:

- Host o nodo: computadoras, servidores, móviles u otros dispositivos finales que consumen y generan datos.
- Router: dispositivo que interconecta redes y enruta paquetes basándose en direcciones IP.
- Switch: conmutador encargado de interconectar dispositivos dentro de una LAN, operando en la capa de enlace.
- Access Point: punto de acceso que permite conectar dispositivos inalámbricos.
- Firewall: dispositivo físico o lógico para filtrar tráfico y aplicar políticas de seguridad.
- Servidor: equipo que provee servicios como DHCP, DNS o aplicaciones empresariales.
- Cableado estructurado: conjunto de cables, paneles y conectores estandarizados que conforman la infraestructura física.

2. Modelo OSI (Open Systems Interconnection)

El modelo OSI divide la comunicación de red en siete capas, permitiendo entender cómo viajan los datos y cómo interactúan los protocolos.

Capa 7: Aplicación
Provee servicios directamente a los usuarios y aplicaciones. Incluye protocolos como HTTP, FTP, DNS y SMTP.

Capa 6: Presentación
Transforma los datos, incluyendo codificación, compresión y cifrado. Tecnologías como SSL/TLS operan aquí.

Capa 5: Sesión
Gestiona el establecimiento, mantenimiento y cierre de sesiones.

Capa 4: Transporte
Transporta datos de extremo a extremo, permitiendo control de flujo, corrección de errores y segmentación. Protocolos principales: TCP y UDP.

Capa 3: Red
Determina rutas, gestiona direcciones IP y maneja el encaminamiento. Incluye IP, ICMP y ARP.

Capa 2: Enlace de Datos
Gestiona el transporte entre nodos directamente conectados. Incluye protocolos como Ethernet, PPP y Wi-Fi.

Capa 1: Física
Incluye medios de transmisión (cable UTP, fibra óptica, radiofrecuencia), voltajes, conectores y señales.

3. Modelo TCP/IP

Es el modelo utilizado en Internet y en la práctica real. Consta de cuatro capas:

- Capa de Aplicación: engloba protocolos como HTTP, DNS, FTP, TELNET.
- Capa de Transporte: define cómo se entregan los datos entre aplicaciones (TCP y UDP).
- Capa de Internet: maneja el direccionamiento y enrutamiento de paquetes (IP, ICMP, ARP).
- Capa de Acceso a Red: define cómo se transmite la información en la red física.

4. Direccionamiento IP

Direcciones IPv4
Una dirección IPv4 está compuesta por 32 bits divididos en 4 octetos. Se expresa en formato decimal separado por puntos.

Clases de direcciones:

- Clase A: destinadas para redes extensas.
- Clase B: usadas para redes medianas.
- Clase C: para redes pequeñas.
- Clase D: tráfico multicast.
- Clase E: uso experimental.

Direcciones especiales incluyen loopback (127.0.0.1), privadas (como 192.168.0.0/16) y broadcast.

Direcciones IPv6
Es un formato de 128 bits expresado en hexadecimal. Ofrece mayor espacio de direccionamiento, autoconfiguración, seguridad integrada e independencia de NAT.

5. Protocolos Relevantes

TCP
Protocolo fiable, orientado a conexión. Incluye mecanismos de retransmisión, segmentación y control de flujo.

UDP
Protocolo sin conexión y más rápido, ideal para comunicaciones en tiempo real como videollamadas o streaming.

ICMP
Utilizado para diagnóstico y envío de mensajes de error. Base de herramientas como ping y traceroute.

ARP
Protocolo fundamental para resolver direcciones IP a MAC en redes locales.

DHCP
Asigna direcciones IP automáticamente a los dispositivos de la red.

DNS
Convierte nombres de dominio a direcciones IP.

6. Comandos de Diagnóstico

Ping
Permite verificar la conectividad, latencia y pérdida de paquetes.

Traceroute
Analiza la ruta que siguen los paquetes hasta su destino.

Ipconfig / Ifconfig
Muestran la configuración de red de un equipo, incluyendo IP, puertas de enlace y DNS.

Nslookup
Herramienta para consultar servidores DNS.

7. Seguridad en Redes

Incluye autenticación, control de acceso, cifrado, firewalls, filtrado de paquetes, IDS/IPS, segmentación y VPN.

8. Tecnologías Inalámbricas

Wi-Fi (802.11)
Incluye estándares como 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac y 802.11ax, operando en bandas de 2.4 GHz y 5 GHz.

Bluetooth, NFC y radiofrecuencia también forman parte de tecnologías inalámbricas actuales.

9. Infraestructura Física

Incluye tipos de cables como UTP, STP y fibra óptica, además de conectores como RJ-45.
Se consideran también racks, patch panels y normativas como TIA/EIA-568.

10. Virtualización y Redes Modernas

Las redes actuales incluyen tecnologías avanzadas:

- VLANs
- SDN (Software Defined Networking)
- VPNs
- Containers y redes Docker
- Cloud Networking

Este documento proporciona una visión ampliada del funcionamiento, componentes y herramientas necesarias para entender las redes informáticas modernas.

SECCIÓN 11. TOPOLOGÍAS DE RED

Las topologías de red representan la forma en que los dispositivos se interconectan física o lógicamente. Comprenderlas permite diseñar redes eficientes, seguras y escalables.

Topología en Bus

Utilizada en redes antiguas con un cable principal donde todos los dispositivos se conectan. Su principal ventaja es su bajo costo, aunque presenta problemas de colisiones y fallos si el cable principal se ve afectado.

Topología en Estrella

La más usada actualmente en redes LAN. Todos los dispositivos se conectan a un punto central, normalmente un switch o un router. Ofrece mayor estabilidad, fácil administración y aislamiento de fallos.

Topología en Anillo

Los nodos forman un circuito cerrado donde los datos viajan de un dispositivo al siguiente. Reduce colisiones y es eficiente, pero un fallo en un nodo puede afectar toda la red si no existe redundancia.

Topología en Malla

Cada dispositivo se conecta con varios otros nodos, generando redundancia y alta disponibilidad. Es utilizada en redes críticas como telecomunicaciones e infraestructuras gubernamentales.

Topología Híbrida

Combinación de dos o más topologías. Flexible, escalable y adaptable a distintas necesidades empresariales.

SECCIÓN 12. REDES VLAN

Las VLAN permiten segmentar una red física en múltiples redes lógicas, mejorando la seguridad y el rendimiento del tráfico.

Funciones principales de una VLAN

- Separación del tráfico por departamentos o roles.
- Reducción de dominios de broadcast.
- Aumento de la seguridad mediante aislamiento de equipos.
- Optimización del rendimiento total del tráfico.

Tipos de puertos en VLAN

- Puerto acceso: pertenece a una única VLAN.
- Puerto troncal (trunk): transporta tráfico de múltiples VLAN usando etiquetado 802.1 Q.
- Puerto híbrido: mezcla de acceso y trunk.

Beneficios de las VLAN en entornos corporativos

Permiten separar servidores, usuarios, voz sobre IP, cámaras de seguridad y sistemas de gestión, creando una estructura aislada y eficiente que reduce el impacto de incidentes de seguridad.

SECCIÓN 13. CONMUTACIÓN Y TABLAS MAC

Los switches aprenden direcciones MAC para enviar los datos únicamente al puerto de destino.

Funcionamiento del aprendizaje MAC

El switch inspecciona cada trama y registra la dirección MAC origen junto con el puerto por donde la recibió. Este registro se almacena en la tabla CAM. Cuando el switch recibe una trama con destino desconocido, la envía por todos los puertos excepto el de origen.

Modos de conmutación

- Store and Forward: revisa la trama completa antes de reenviarla.
- Cut Through: reenvía apenas identifica la dirección destino.
- Fragment Free: espera un tamaño mínimo para evitar colisiones tardías.

SECCIÓN 14. ENRUTAMIENTO Y PROTOCOLOS DINÁMICOS

El enrutamiento permite enviar paquetes entre redes distantes. Puede hacerse de forma estática o dinámica.

Enrutamiento estático

Requiere configuración manual de rutas. Es sencillo y seguro, pero no escala bien en redes grandes.

Protocolos de enrutamiento dinámico

- RIP: usa algoritmo de vector distancia, limitado en redes grandes.
- OSPF: protocolo de estado de enlace, altamente escalable.
- EIGRP: híbrido, exclusivo de Cisco, eficiente y rápido.
- BGP: protocolo que controla el enrutamiento global de Internet.

Conceptos importantes en enrutamiento

- Métrica: valor usado para decidir la mejor ruta.
- Vecinos: routers adyacentes que intercambian información.
- Convergencia: tiempo en que todos los routers tienen la misma información de red.

SECCIÓN 15. NAT (TRADUCCIÓN DE DIRECCIONES)

NAT permite que múltiples dispositivos de una red privada utilicen una única dirección IP pública para acceder a Internet.

Tipos de NAT
• NAT estático: una IP privada se mapea a una IP pública fija.
• NAT dinámico: hay un grupo de IP públicas que pueden usarse según disponibilidad.
• PAT o NAT sobrecargado: múltiples dispositivos comparten la misma IP pública usando puertos distintos.

Ventajas
• Ahorro de direcciones IPv4 públicas.
• Capa adicional de seguridad al ocultar IP internas.
• Flexibilidad para redes corporativas y de hogar.

SECCIÓN 16. FIREWALLS Y SEGURIDAD PERIMETRAL

El firewall actúa como un filtro que controla qué tráfico puede entrar o salir de la red.

Tipos de firewalls
• De filtrado básico de paquetes.
• De inspección con estado (Stateful).
• Firewalls de aplicación (WAF).
• Firewalls de próxima generación (NGFW).

Características comunes
• Control de acceso.
• Prevención de intrusiones.
• Registros y auditoría.
• Inspección profunda de paquetes.
• Herramientas de geobloqueo y bloqueo por reputación.

SECCIÓN 17. WIFI Y 802.11

La tecnología Wi-Fi es fundamental en los entornos modernos.

Estándares Wi-Fi

• 802.11b: 11 Mbps en 2.4 GHz.802.11g: 54 Mbps en 2.4 GHz.
• 802.11n: hasta 600 Mbps en 2.4 y 5 GHz.
• 802.11ac: gigabit inalámbrico en 5 GHz.
• 802.11ax (Wi-Fi 6): optimización para ambientes densos y alta eficiencia.
• Wi-Fi 6E: añade la banda de 6 GHz.

Conceptos avanzados

• Beamforming: concentración de señal hacia el cliente.
• MU-MIMO: múltiples transmisiones simultáneas.
• Roaming: movimiento entre puntos de acceso sin perder conexión.
• Canales y ancho de banda: 20/40/80/160 MHz.

SECCIÓN 18. REDES WAN Y TECNOLOGÍAS DE ACCESO

Las redes WAN permiten interconectar sucursales, empresas y ciudades completas.

Tecnologías comunes

• MPLS: red privada de alta calidad usada en entornos corporativos.
• Metro Ethernet: despliegues de fibra óptica.
• Enlaces satelitales: cobertura en áreas remotas.
• LTE/5G: conexiones móviles empresariales.
• VPN site-to-site: conexión segura entre sedes mediante Internet.

SECCIÓN 19. MONITOREO Y ANALÍTICA DE RED

El monitoreo permite detectar fallas, amenazas y congestión antes de que afecten a los usuarios.

Herramientas y métodos
• SNMP: protocolo de gestión de dispositivos.
• Syslog: envío centralizado de registros.
• NetFlow y sFlow: análisis de tráfico.
• Herramientas como Zabbix, PRTG, Grafana, Wireshark.

Parámetros importantes
• Latencia.
• Jitter.
• Pérdida de paquetes.
• Uso de CPU y memoria.
• Congestión en enlaces.

SECCIÓN 20. REDES DEFINIDAS POR SOFTWARE (SDN)

SDN separa el plano de control del plano de datos, permitiendo una administración centralizada.

Ventajas
• Automatización.
• Reducción de errores humanos.
• Configuración dinámica.
• Integración con sistemas basados en IA.